AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Anthony Fry, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **1148 East 222nd Street, Euclid, Ohio 44117**, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B, and to seize same.

2. I have been a Special Agent with the FBI since September 2018. I am currently assigned to an FBI squad which investigates securities fraud, wire fraud, and other financial crimes. During my tenure with the FBI, I have participated in financial fraud investigations involving stock market manipulation and other illegal manipulative trading schemes. I have participated in all aspects of investigations including executing search warrants, debriefing defendants and informants, interviewing witnesses, and reviewing and analyzing recorded interstate telephone conversations. As part of my official law enforcement duties, I have participated in the execution of search warrants involving, among other things, the search and seizure of computers, computer equipment, software, and electronically stored information.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 15, United States Code, Sections 78j(b), 78ff; Title 17, Code of Federal Regulations, Section 240.10b-5, and Title 18, United States Code, Section 371 have been committed by PAUL SPIVAK, and others, known and unknown. There is also probable cause to search the PREMISES described in Attachment A for evidence, instrumentalities, contraband, or fruits of these crimes as further described in Attachment B.

Relevant Regulatory Principles and Definitions

5. The United States Securities and Exchange Commission, hereinafter referred to as the SEC, was an independent agency of the Unites States which was charged by law with protecting investors by regulating, and monitoring, among other things the purchase, and sale of publicly traded securities, including securities traded on the United States based stock exchanges.

6. Federal securities law, and regulations prohibited fraud in connection with the purchase, and sale of securities, including the use of false and misleading statements and the failure to disclose material information to: (a) the SEC in publicly available filings; (b) brokerage firms, and transfer agents involved in the purchase, and sale of stock in companies subject to SEC regulation; and (c) the public. Federal securities laws and regulations also prohibited the manipulation of stock through, among other things, sales made at the times and at prices set by those trading the stock rather than by market forces.

7. Title 15, United States Code, Section 78j(b) makes it a federal offense for any person directly, or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of a national securities exchange, to use or employ, in

connection with the purchase or sale of any security registered on a national exchange, any manipulative, or deceptive device or contrivance in contravention of such rules and regulations as the SEC may prescribe as necessary or appropriate in the public interest of for the protection of investors, including: (a) employing devices, scheme, and artifices to defraud; (b) making untrue statements of fact or omitting to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and (c) engaging in acts, practices, and courses of business which operated as a fraud upon investors, in connection with the purchase and sale of the securities. Failure to disclose to investors commission payments from third parties, including payments from issuers, was considered an omission of a material a fact as part of a securities transaction.

8. Title 18, United States Code, Section 371 (Conspiracy to commit securities fraud) two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy.

9. An over-the-counter market ("OTC") is a decentralized market in which market participants trade stocks, commodities, currencies, or other instruments directly between two parties and without a central exchange or broker. OTC markets do not have physical locations, but instead trading is conducted electronically. In an OTC market, dealers act as market-makers by quoting prices at which they will buy and sell a security, currency, or other financial product. A trade can be executed between two parties in an OTC market without others being aware of

the price at which the securities transaction was completed. OTC markets are typically less transparent than exchanges and are also subject to fewer regulations.

10. "Microcap" or "penny" stocks referred to stocks of publicly traded United States companies which had low market capitalization. Microcap stocks were subject to price manipulation because they were thinly traded and subject to less regulatory scrutiny than stocks that were traded on notable exchanges such as the National Association of Securities Dealers Automated Quotes ("NASDAQ"), and the New York Stock Exchange ("NYSE"). The NASDAQ, and NYSE had specific standards that were monitored and enforced for a company to have its stock traded on those exchanges. Additionally, large blocks of these type of stocks were often controlled by a small group of individuals, which enabled those in the group to control and orchestrate manipulative trading in those stocks.

Market Manipulation Schemes

11. A pump and dump scheme was a securities fraud scheme that typically involved the artificial inflation of the stock price of a publicly traded company (the "pump") so that individuals who control a substantial portion of the company's stock can sell shares of that stock at artificially high prices to other investors (the "dump") in the open market. Generally, pump and dump schemes effected the artificial inflation in stock share price by, among other things, issuing new releases, and promotional materials regarding the company, and its stock. These press releases often contain false, misleading, or exaggerated information, and are timed for the greatest enrichment of the individuals who control a substantial portion of the company's stock.

In addition, pump and dump schemes engage in manipulative trading of the stock to affect its share price and generate the appearance of demand for the stock shares.

12. As a result of a pump and dump independent third-party purchasers were subsequently left with a near worthless security when the price dropped to accurately reflect the stocks true value, or lack thereof, in the open market. There were generally three phases to a pump and dump scheme; (a) first, obtaining and concealing control of a significant portion of a publicly traded company's stock, (b) second, fraudulently inflating or keeping inflated the price, and trading volume of the company's stock through a variety of means, and (c) third, once the price of the stock was fraudulently inflated, selling the stock using the fraudulently inflated price as a benchmark, thereby, profiting at the expense of the investing public.

Rule 144 Schemes

13. Federal statutes and regulations generally prohibit a company or its affiliates from selling shares of stock to the investing public unless the company makes public disclosures about its ownership, management, finances and operations. Such disclosures usually are made by filing a registration statement with the SEC for a particular stock distribution.

14. There are, however, exemptions from the registration requirements. One exemption involves the distribution of stock pursuant to Rule 144 under the Securities Act of 1933. As long as a person is not an affiliate of the company or its management, and has cleared various technical hurdles, that person may legally sell the stock under Rule 144. In contrast, an affiliate, defined as a person who "directly, or indirectly through one or more intermediaries, controls or is controlled by, or is under common control" with those who manage the company,

is subject to additional restrictions. Relevant to Rule 144, affiliates are allowed to sell shares to the public only if they meet a number of requirements, including (1) filing disclosures with the SEC (on SEC Form 144) regarding the sales, and (2) staying within strict share volume limitations. The volume limitations restrict a person's sales under Rule 144 during any three-month period to (a) 1% of the total number of outstanding shares, or (b) the average weekly trading volume for the preceding four weeks, whichever is greater.

15. I also know through my training and experience, and through consultation with other agents, investigators, and regulators, that fraudulent schemes to evade these restrictions are common. This is particularly true with respect to the stock of microcap companies. In such schemes, an individual who is a known affiliate of a microcap company (the "Insider," e.g., the company's CEO, CFO, or member of its board of directors) enters into a secret agreement with another individual who has access to a brokerage account (the "Seller"). Under such an agreement, the Insider transfers or issues stock (or a security that can be converted into stock) to the Seller. The Seller then attempts to deposit the stock at his or her brokerage firm. Under applicable securities regulations, brokerage firms have a duty of reasonable inquiry to determine whether a client's (in this example, the Seller's) offering of stock to the public is registered with the SEC or an exemption applies.

16. If the Seller is successful in convincing the brokerage firm that an exemption from the registration requirement applies, the Seller sells the stock to the public, and kicks back a portion of the proceeds to the Insider. This secret agreement, if known, would support a finding that the Seller is him or herself an "affiliate," and therefore could only sell a limited quantity of

shares to the public. The affiliate and the Insider therefore often misrepresent the facts surrounding the arrangement to, and hide the secret agreement from, the Seller's brokerage firm.

17. Defendants, Relevant Persons, Entities, and Financial Accounts

18. PAUL SPIVAK was a resident of Ohio.

19. OLGA SMIRNOVA was a resident of Ohio

20. CHARLES SCOTT was a resident of Virginia.

21. FORREST CHURCH was a resident of Alabama.

22. RICHARD MALLION was resident of Florida.

23. THOMAS COLLINS was a resident of Texas.

24. HUGHE DUWAYNE GRAHAM was a resident of California. GRAHAM also utilized the name JOHN MORGAN.

25. CHRISTOPHER BONGIORNO was a resident of Ohio. BONGIORNO also utilized JOHN POWERS.

26. JASON ARTHUR was a resident of Nevada. ATHURS also utilized the name JIM GATES.

27. DONALD LEE HOWARD was a resident of Nevada.

28. LARRY LOUIS MATYAS was a resident of Nevada.

29. US LIGHTING GROUP, INC., ("USLG"), was a publicly traded Florida corporation, and was registered on or about October 17, 2003, with its principal place of business in Euclid, Ohio. PAUL SPIVAK was the Chief Executive Officer of USLG. USLG's purported business operations were focused on the design and manufacturing of commercial LED lights,

aftermarket automotive parts, and the design and manufacturing of fiberglass recreational campers and boats. US LIGHTING GROUP, INC. traded on OTC Markets under the ticker USLG.

30. On or about October 15, 2002, SPIVAK opened an account at PayPal in the name of Intellitronix ending in x8170.

31. On or about February 10, 2014, SPIVAK and SMIRNOVA opened a joint checking account in the name of themselves at JPMorgan Chase ending in x7373.

32. On or about February 25, 2015, SPIVAK opened a bank account at Home Savings and Loan Company, now called Premier Bank, in the name of SPIVAK ending in x3705.

33. HDG GLOBAL MARKETING, LLC ("HDG GLOBAL"), was registered on or about October 11, 2018, as a California limited liability company with its principal place of business in Corona, California. GRAHAM and Erika Graham. were listed as the members, and manager of HDG GLOBAL. On or about May 30, 2019, GRAHAM, and Erika Graham opened bank account number x5003 at JP Morgan Chase Bank in the name of HDG GLOBAL MARKETING, LLC

34. On or about November 18, 2016, BONGIORNO opened an account at Bank of America in the name of NORTH STAR ASSETS, LLC ("NORTH STAR") ending in x9235. BONGIORNO was the only signatory on the account.

The Fraudulent Schemes

35. The investigation revealed that SPIVAK utilized nominees to conceal his beneficial ownership in free trading shares held in the name of SCOTT and CHURCH in

violation of securities laws. SPIVAK failed to disclose his beneficial ownership, influence and control of the shares owned by SCOTT and CHURCH to the investing public and the SEC. Moreover, SPIVAK knowingly utilized the sale of free-trading shares to raise operating capital for USLG.

36. SPIVAK hired unregistered brokers to solicit the investing public to purchase both restricted and free-trading shares of USLG. The unregistered brokers solicited investors, often made misrepresentations regarding USLG, the nature and terms of the investment and failed to disclose the brokers was to receive a commission on the investor's purchase which often was 30% to 40% of investment.

37. SPIVAK conspired to have FBI Undercover Employees ("UCEs") actively promote USLG's stock by coordinating the issuance of press releases by USLG with a planned promotional program. SPIVAK engaged in the scheme in in hopes of raising the share price and trading volume in USLG's stock and for personal enrichment. During the course of the scheme, SPIVAK arranged the sale of free-trading shares from nominees to the UCEs for the purpose of the market manipulation scheme.

38. SPIVAK knowingly opened PayPal accounts in the name of USLG to sell the Company's products and merchandise through online forums or platforms. SPIVAK knowingly took the proceeds and sales from the online forums and platforms and transferred the proceeds directly to personal accounts opened and controlled by SPIVAK. SPIVAK used the proceeds for personal expenses and self-enrichment.

Probable Cause

Use of Unregistered Brokers to Solicit Investors

39. As previously mentioned, SPIVAK hired unregistered brokers to solicit the investing public to purchase both restricted and free-trading shares of USLG.

40. On or about February 28, 2020, BONGIORNO and ARTHUR, were charged in the United States District Court for the Northern District of Ohio by the SEC for soliciting investors to purchase shares of USLG and another stock from September 2015 to November 2018 (Case No. 1:20cv469). BONGIORNO and ARTHUR were not registered brokers or associated with a registered broker-dealer. BONGIORNO and ARTHUR received approximately 40% to 50% commissions from the investors share purchases.

41. According to the SEC complaint, BONGIORNO and ARTHUR engaged in fraud by lying to USLG and investors about their identities and recruiting and paying other unlicensed individuals to engaged in securities solicitations. The SEC further alleged ARTHUR lied to an investor about his compensation and BONGIORNO misappropriated investor funds.

42. On or about November 6, 2020, GRAHAM, MATYAS, and HOWARD, were charged in the United States District Court for the Northern District of Ohio by the SEC for soliciting investors to purchase shares of USLG from October 2017 to May 2019 (Case No. 1:20cv2505). GRAHAM, MATYAS, and HOWARD were not registered brokers or associated with a registered broker-dealer. GRAHAM, MATYAS, and HOWARD received approximately 40% commissions from the investors share purchases.

43. As part of the investigation FBI Agents interviewed Victim-1. Victim-1 invested approximately $125,000 in USLG. Victim-1 identified speaking to a number of individuals from USLG regarding his/her investments into USLG, including JOHN MORGAN, DON HOWARD,

RICHARD BURNS, JACOB ROSEN, CHRIS Last Name Unknown ("LNU"), SCOTT KOLNICH, and MARIA DANIEL. BURNS later identified himself to Victim-1 as MALLION. Victim-1 stated that none of the representatives from USLG disclosed that they would be compensated in any manner from Victim-1's investment. Victim-1 was told their investment would be used to expand the company and make acquisitions.

44. From on or about November 9, 2017, to on or about January 2, 2019, GRAHAM received approximately $440,627.24 in commissions from USLG's Huntington bank account ending in x5817 following investments made by investors. The funds were deposited into a joint checking account controlled by GRAHAM and GRAHAM's HDG GLOBAL MARKETING LLC business bank account.

45. From on or about December 26, 2017, to on or about April 19, 2018, BONGIORNO received approximately $132,688.25 in commissions from USLG's Huntington bank account ending x5187 following investments made by investors. The funds were deposited into BONGIORNO's NORTH STAR business bank account.

46. From on or about July 8, 2016, to on or about May 8, 2018, ARTHUR received approximately $583,508.25 in commissions from USLG's Huntington bank account ending in x5187 following investments made by investors. The funds were deposited into accounts held by A&M Lead Consulting LLC and US Lead Generation, which were controlled by ARTHUR.

47. From on or about May 24, 2018, to on or about May 29, 2019, MATYAS received approximately $362,916.40 in commissions from USLG's Huntington bank account ending in x5187 following investments made by investors. The funds were deposited into a

combination of personal and business accounts including the business Secured Consulting, controlled by a nominee of MATYAS.

48. FBI Agents interviewed GRAHAM in August of 2020 following the arrest of GRAHAM on a separate securities fraud case pending in the Northern District of Ohio (1:20cr842). According to GRAHAM, he made approximately $100,000 working on the USLG deal and paid the rest of the money received into his (GRAHAM's) bank account to others. GRAHAM created HDG Global Marketing for the work he was doing for USLG. SPIVAK and Susan Tubbs started the process of creating the entity for GRAHAM. GRAHAM stated BONGIORNO was a stock promoter from Ohio who worked on USLG and other stocks. GRAHAM stated that ARTHUR also called investors to sell them USLG stock. GRAHAM stated some of the individuals who sold USLG stock to investors, and to whom GRAHAM paid for the sales, were GRAHAM's friends whom he did not want to see get in trouble. GRAHAM stated SPIVAK had control of free-trading shares in USLG that were not in SPIVAK's name. GRAHAM stated the shares were in MALLION's name and MALLION also sold shares of USLG. GRAHAM understood SCOTT to be an investor that loaned SPIVAK money and controlled a large amount of free-trading stock in USLG. GRAHAM acknowledged the point of speaking with investors was to talk the investors into buying shares in USLG so that SPIVAK, MALLION and SCOTT could make money by selling shares.

Involvement of RICHARD MALLION in USLG

49. RICHARD MALLION was previously charged in 1996 by the SEC as part of a stock promoter, undisclosed commission/kickback scheme. MALLION consented to the entry of a final judgment without admitting or denying the allegations from the complaint by the SEC and

received a penny stock bar from participation in future penny stock offerings and ordered MALLION to pay $100,000 in disgorgement.

50. On or about October 10, 2019, MALLION, was charged in the United States District Court for the Southern District of Florida again by the SEC. MALLION was charged with conduct from May 2016 through at least October 2018, as MALLION "actively solicited individuals throughout the United States to invest in the securities of microcap issuers Virtual MediClinic USA LLC and US Lighting Group, Inc (f/k/a The Luxurious Travel Corporation)."

51. According to the SEC complaint, MALLION, as an unregistered broker made material misstatements to investors and earned transaction-based compensation generally in the amount of 40% of the investment proceeds in relation to USLG stock.

52. On or about October 14, 2019, MALLION consented to the entry of a final judgment in the United States District Court for the Southern District of Florida, without admitting or denying the allegations from the complaint by the SEC. As part of the agreement MALLION was ordered a disgorgement of $634,510.63 which represented the profits gained as a result of MALLION's conduct.

53. In October 2020, FBI agents interviewed MALLION for this investigation. MALLION stated he had known SPIVAK for many years. MALLION made an agreement with SPIVAK on USLG in which MALLION received a large portion of free trading stock in USLG. MALLION hired TOM COLLINS to promote USLG in order to increase USLG's share price and trading volume. MALLION paid COLLINS using proceeds of MALLION's USLG stock sales. MALLION stated that at that time, SPIVAK was aware of the arrangement and wanted

50% of the stock proceeds generated from the sale of USLG shares. MALLION refused to pay SPIVAK as part of the illicit arrangement. MALLION also stated that as the stock began to increase in price and volume, CHURCH and SCOTT purchased the remaining free-trading shares in USLG.

54. MALLION sold approximately $600,000 worth of free-trading shares of USLG, as COLLINS helped arrange trades in the open market. COLLINS told MALLION the share price and number of shares to place trades at in the market, commonly known as match trading. These trades were a way to arrange trades with investors that COLLINS had solicited. COLLINS told MALLION how to trade USLG shares via telephone calls and text messages.

55. The SEC deposed SPIVAK as part of its investigation of MALLION. On or about July 30, 2019, in the Northern District of Ohio, Eastern Division, while under oath SPIVAK answered the SEC's questions regarding USLG, undisclosed commissions, unregistered brokers, specifically MALLION, COLLINS, and financial statements and purchases related to USLG and INTELLITRONIX.

56. As part of his testimony, SPIVAK discussed the involvement of MALLION and free-trading shares of USLG. When SPIVAK and MALLION made an agreement to purchase USLG, the deal involved the purchase of 25,000,000 restricted shares, and 5,000,000 shares of free-trading stock. SPIVAK stated he could not be involved with free-trading shares in USLG due to legal restrictions and described it as a "Chinese wall" that was serious and not to be violated. SPIVAK acknowledged that MALLION arrived at a deal to purchase the free-trading shares of USLG. SPIVAK acknowledged there was a verbal agreement between MALLION and

SPIVAK that MALLION would sell free trading shares in his (MALLION) control, and MALLION would use the proceeds to buy newly issued restricted shares directly from the company. SPIVAK acknowledged a verbal agreement with MALLION in violation of United States securities laws that MALLION would use the sales of free trading USLG stock to raise capital and reinvest into USLG for newly restricted shares.

Conversations with Undercover Agents and the Cooperating Witness

57. On or about February 15, 2021, Undercover Employee-1, ("UCE-1"), and a cooperating witness ("CHS-1")[1] had a consensually recorded in-person meeting with SPIVAK and SMIRNOVA in the Fort Lauderdale, Florida area. UCE-1 portrayed an investor. During the meeting SPIVAK described a scheme where UCE-1, CHS-1, and their associates, purchase shares of USLG, sell the shares and use the money to purchase more shares from USLG. SPIVAK stated "what you are supposed to do, is sell it, buy more stock and we keep going in a circle like that." Regarding a scenario where UCE-1 and CHS-1 purchase stock directly from SPIVAK and that Company for $0.50 per share and sell the shares for $1.00 per share and then buy more shares for $0.50 per share, SPIVAK responded "yes, yes, yes, that is what everybody

[1] CHS-1 was previously charged and convicted of securities fraud and agreed to cooperate with law enforcement in hopes of reducing his sentence pursuant to U.S.S.G. § 5K1.1. After serving their sentence, CHS-1 continued to cooperate with law enforcement. I believe CHS-1 was and is a reliable and credible source of information as the information CHS-1 provided has been corroborated by independent investigation.

has been doing." SPIVAK added "that's how we make a bunch of money" and that by doing this, SPIVAK has a never-ending supply of money coming into the company.

58. On or about February 16, 2021, CHS-1 had a consensually recorded in-person meeting with SPIVAK, and SMIRNOVA. SPIVAK told CHS-1 that all the convertible notes had been converted in USLG except for one. SPIVAK stated if CHS-1 purchased the note from the investor that held the note, SPIVAK could issue a press releases stating all the notes had been converted. SPIVAK told CHS-1 that during the previous scheme he executed to manipulate the stock USLG's stock price went up to $1.50 per share. SPIVAK described his previous partner as a "professional pump and dumper."

59. On or about March 5, 2021, Undercover Employee-2 ("UCE-2"), and CHS-1 had a consensually recorded in-person meeting with SPIVAK, and SMIRNOVA at the PREMISES. UCE-2 portrayed a wealthy investor interested in purchasing shares of USLG. During the meeting SPIVAK told SMIRNOVA to "go in and grab the top-secret document and bring it in here." SPIVAK stated he would tell UCE-2 and CHS-1 how they were going to make money with the stock, and that SPIVAK was happy there was not many people in the room for the conversation. SPIVAK showed UCE-2 and CHS-1 a copy of the most current financial statements which were not available to the public yet. SPIVAK told CHS-1 and UCE-2 that he had two individuals who were "very trusted friends" and held approximately 3 million USLG shares each. SPIVAK stated the plan was, once the stock price rose, the two individuals would sell off the stock and buy more stock from the company. SPIVAK stated the two individuals would not sell the stock for $0.15 per share and the purchase price would likely be higher than

the open market price. SPIVAK stated the shares were technically company stock, but if the company owned the stock, it would no longer be free-trading shares. SMIRNOVA stated one individual was in Virginia, and the other was in Alabama. SPIVAK stated there was very little stock in the float and it would not take much to get the stock price to "go very high". I know from my training and experience that the "float", is the number of shares publicly available in the market for investors to trade in a stock and that SPIVAK was telling UCE-2 and CHS-1 given the small size of stock available for the public to trade in USLG made it easier for SPIVAK, UCE-2 and CHS-1 to manipulate USLG's share price.

60. On or about March 10, 2021, CHS-1 had a consensually recorded telephone call with SPIVAK. SPIVAK and CHS-1 agreed to start with a $25,000 transaction as a "test" with each of SPIVAK's "trusted guys", and to later negotiate the purchase the remainder of the six million shares. SPIVAK told CHS-1 that SPIVAK needed to call his co-conspirators and inform them CHS-1 was "on the team" and not an "outsider" prior to negotiating the share purchases. Later that day, SPIVAK called CHS-1 and stated he would text CHS-1 the contact information for SCOTT and that SCOTT was awaiting CHS-1's call regarding purchasing shares of USLG. SCOTT also controlled another publicly traded company that SPIVAK gave to SCOTT. SPIVAK stated after they made a bunch of money on USLG's stock they could move to SCOTT's public company.

61. On or about March 10, 2021, CHS-1 had a consensually recorded telephone call with SCOTT. SCOTT told CHS-1 that SCOTT had approximately 3,500,000 shares of USLG and was willing to sell the shares.

62. On or about March 15, 2021, CHS-1 had a consensually recorded telephone call with CHURCH. CHURCH told CHS-1 that the arrangement CHURCH maintained with SPIVAK worked out "fairly well for [SPIVAK]" and had not "totally sucked" for CHURCH. CHURCH told CHS-1 that he had approximately $200,000 currently invested in USLG, owned approximately 1,800,000 USLG shares in certificate form, book form at the transfer agent and in several brokerage accounts controlled by CHURCH.

63. On or about March 16, 2021, CHS-1 had a consensually recorded telephone call with SPIVAK. SPIVAK told CHS-1 that SCOTT did not sign the stock purchase agreement because the agreement showed $0.25 per share for the sale and not $0.30 per share. SPIVAK stated that SCOTT and CHURCH were "holding onto the stock for me" or holding the stock for the company. SPIVAK stated that prior to CHS-1's involvement, SCOTT and CHURCH were going to run a promotion with USLG after the audited financial statements were completed. SPIVAK stated that SCOTT and CHURCH "basically got the stock for free" so they would have to pay tax on the entire $0.30 per share, and then send SPIVAK $0.15 per share. SPIVAK stated he trusted SCOTT and CHURCH like family, and that was why SCOTT and CHURCH were "holding on to the corporate, free-trading stock."

64. On or about March 16, 2021, CHS-1 had a consensually recorded telephone call with SCOTT. During the call, SCOTT agreed to sign and return a stock purchase agreement to sell a block of 100,000 free-trading shares of USLG to UCE-2 for $0.25 per share.

65. On or about March 24, 2021, CHS-1 had a consensually recorded telephone call with CHURCH. During the call, CHURCH stated that he expressed concern to SPIVAK that

after CHURCH received the $25,000 from CHS-1, and paid SPIVAK $15,000 and taxes on the stock sale, CHURCH was not even going to clear $10,000. CHURCH stated that the original deal with SPIVAK was that CHURCH and SCOTT would receive their original $50,000 investments back before sending money to SPIVAK, but that did not happen.

66. On or about March 26, 2021, the FBI sent an interstate wire transfer of $25,000 from an FBI controlled bank account to CHURCH's Bank of America account ending in x2853 in the name of CHURCH which was located in Haleyville, Alabama for the purchase of 100,000 free-trading shares of USLG.

67. On or about March 30, 2021, UCE-2 and CHS-1 had a consensually recorded in person meeting with SPIVAK in Cleveland, Ohio. During the consensually recorded in person meeting with SPIVAK, UCE-2 and CHS-1 initiated a Zoom call with Undercover Employee-3 ("UCE-3"). UCE-3 portrayed a stock promoter. SPIVAK stated there is approximately 6 million shares of USLG in "very friendly hands," and further discussed running a promotion to increase USLG's stock price. SPIVAK told CHS-1 and UCE-2 that SCOTT and CHURCH considered running a promotion before with USLG and that SCOTT and CHURCH would do whatever SPIVAK says because "they're very trusted guys." SPIVAK went on to say that was why SCOTT and CHURCH were the "friendly hands" holding onto the stock in order to prevent the stock from becoming restricted.

68. On or about April 1, 2021, the FBI sent an interstate wire transfer of $25,000 from an FBI controlled bank account to SCOTT's Navy Federal Credit Union account ending in x4974 for the purchase of 100,000 free-trading shares of USLG.

69. On or about April 2, 2021, CHURCH sent a $15,000.00 wire transfer from a CHURCH controlled Bank of America account ending in x2853 to USLG's Huntington bank account ending in x5187.

70. On or about April 13, 2021, CHS-1 had a consensually recorded telephone call with SPIVAK. SPIVAK told CHS-1 that SPIVAK could not wait around anymore and that he had "perfectly good press releases that are being wasted." SPIVAK stated he was starting a marketing campaign that week. SPIVAK was going to call "the guys" and ask why they had not sent the stock certificates to CHS-1.

71. On or about April 15, 2021, CHS-1 had a consensually recorded telephone call with CHURCH. CHURCH stated he had transferred the share to CHS-1 at the transfer agent in book form. CHURCH stated he had moved an additional 800,000 share to book form at the transfer agent to sell to CHS-1 and CHS-1's associates in the future.

72. On or about April 16, 2021, CHS-1 had a consensually recorded telephone call with SPIVAK. SPIVAK told CHS-1 that SPIVAK was selling Intellitronix for $4,500,000. SPIVAK stated he would not take the money to pay off his $3,000,000 in debt. SPIVAK was going to utilize the money to meet the requirements to move to NASDAQ, except for the share price. SPIVAK stated he needed CHS-1 and CHS-1's associates to help get the share price up to $3.00 per share or SPIVAK would have reverse split the stock. SPIVAK told CHS-1 to tell the news to UCE-2, but nobody knew what was going on. SPIVAK stated he could not be involved in free-trading stock which is why the stock was with SCOTT and CHURCH SPIVAK later

added that "we are all working together as a team" and if SPIVAK was involved with the free-trading stock it would become restricted and "it's just lost all of its value."

73. On or about April 19, 2021, CHS-1 had a consensually recorded telephone call with SPIVAK. During the call, SPIVAK asked for a target date for when the promotion was going to start on USLG. SPIVAK described himself as the "press release king" and asked CHS-1 to ask UCE-1 how many press releases UCE-1 wants and by what date. SPIVAK asked CHS-1 to have UCE-1 call SPIVAK to discuss the timing of the promotion and press releases.

74. On or about April 22, 2021, CHS-1 had a consensually recorded telephone call with SPIVAK. SPIVAK told CHS-1 that SPIVAK only had access to restricted shares to provide to UCE-2. Regarding the possibility of issuing consulting shares to UCE-2, SPIVAK stated "I'm sure we can work something out." SPIVAK told CHS-1 not to email SPIVAK or put anything in writing.

75. On or about May 7, 2021, CHS-1 had a consensually recorded telephone call with SPIVAK. SPIVAK confirmed with CHS-1 that the promotion of USLG would begin in June.

76. On or about May 18, 2021, CHS-1 had a consensually recorded in-person meeting with SPIVAK at the PREMISES. While discussing USLG's projected share price, SPIVAK told CHS-1 that everything he and CHS-1 were discussing was "only with you and I (SPIVAK) in the room." Later in the meeting, SPIVAK told CHS-1 that they needed to come up with a plan and that SPIVAK would compensate CHS-1 "for when X happens... and nobody f**king knows about it, not even my wife." As SPIVAK started to formalize a plan to compensate CHS-1, SPIVAK directed CHS-1 to take a walk with him outside and to leave his cell phone in the office

so their conversation could not be recorded. As SPIVAK and CHS-1 departed USLG's office, SPIVAK asked CHS-1 what percentage of the 6 million shares CHS-1 wanted as compensation. SPIVAK told CHS-1 that he would have to give it to CHS-1 "as a consultant." SPIVAK further stated, "I will give you 1.5 million shares if they (UCE-2 and UCE-3) buy them (SCOTT and CHURCH) out completely." SPIVAK and CHS-1 continued to discuss a plan to compensate CHS-1 and agreed to draft up a consulting agreement between USLG and a name of a to-be-determined consulting company.

77. On the same date, during the consensually recorded in-person meeting with SPIVAK, SPIVAK raised coming up with a cover story if SPIVAK and CHS-1 were questioned by authorities. SPIVAK told CHS-1 that they should assume they would "get busted," and asked CHS-1 what they would say "when they get busted." SPIVAK told CHS-1 that if they assumed they were going to get caught, then when they did, it would not be a problem. SPIVAK asked CHS-1 if he had an iPhone and instructed CHS-1 to FaceTime him if CHS-1 "needed to tell me (SPIVAK) something" because "you can't listen in." SPIVAK subsequently stated that what he and CHS-1 were doing was "against SEC rules." SPIVAK further discussed CHS-1's compensation being through a consulting agreement between USLG and CHS-1. The discussion between CHS-1 and SPIVAK ended by way of a handshake agreement.

US Lighting Group PayPal Account

78. As part of SPIVAK's deposition on July 30, 2019, SPIVAK testified about eBay and PayPal accounts. SPIVAK, while under oath, made false statements concerning the proceeds from the sale of Intellitronix products, then an operating subsidiary of USLG. The SEC attorney

asked SPIVAK the following question, "so products sold, the purchaser makes a payment, say by PayPal for the product. Where does the money go?" SPIVAK responded, "Goes to PayPal, and eventually we put it into the Intellitronix bank account, and it's reported on the financials." In his testimony, SPIVAK stated USLG utilized QuickBooks to track the daily financial activity of USLG and Intellitronix.

79. I know from reviewing financial records that the Intellitronix PayPal account ending in x8170 was used to receive funds from the sale of products related to Intellitronix and USLG. From on or about September 9, 2015, to on or about March 3, 2021, SPIVAK made or caused to made 141 transfers, amounting to approximately $1,167,794.84, from the PayPal account to SPIVAK's personal accounts ending in x7373 and x3705. That money remained in SPIVAK's personal accounts. The following table shows the number of transfers and the approximate amount received in each account during the aforementioned date range:

Account	Account Holder	No. of Transfers	Total Approx. Amount
JP Morgan Chase x7373	SPIVAK & SMIRNOVA	66	$430,097.75
Premier Bank X3705	SPIVAK	75	$737,697.09

Description of the Premises

80. On or about May 18, 2021, an FBI agent observed the business address of **1148 East 222nd Street, Euclid, Ohio 44117**, the PREMISES, as a single-story office building with a larger rear warehouse connected to the front single-story office space. On the same date, CHS-1 met with SPIVAK at the PREMISES and recorded the meeting. CHS-1 observed that the front entrance faced East 222nd street and the main front door opened into a foyer area with a locked

security door. The security door required key code access or an individual present inside the office space to manually open the door from inside. The single-story office space had a series of cubicles at the front end of the single-story office space that contained multiple computers and USLG-related paperwork. CHS-1 entered through the front main door. CHS-1 stated that upon entry from the front door, on the opposite wall from the cubicles were several enclosed office spaces for the Chief Financial Officer and Director of Sales. CHS-1 reported that there was a conference room that containing a whiteboard and computer in the center of the single-story office area, and behind the cubicles and enclosed office spaces. According to CHS-1, SMIRNOVA's and SPIVAK's private office space was next to the conference room. This private office space shared a common wall with the conference room. SPIVAK's office had its own door. CHS-1 reported that behind the single-story office space was a lunchroom and an open warehouse area. The warehouse area had a staircase leading up to a separate office that overlooked the warehouse. CHS-1 reported SPIVAK walked down the staircase to greet CHS-1. CHS-1 reported computers and USLG paperwork in the open warehouse area. CHS-1 also reported numerous motorcycles, automobiles, and electronics associated with USLG in the warehouse area.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

81. As described above and in Attachment B, this application seeks authority to search for, and seize, records likely to be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer hard drive or forms of electronic other storage media. Thus, the warrant applied for would authorize the

seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

82. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe records and other information constituting evidence, fruits and instrumentalities of the violations under investigation will be stored on computers or other electronic storage medium, for the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on a review of other evidence related to this investigation, spreadsheets, financial records, invoices, bank records and statements, correspondence, public filings, corporate documents including records related to stock transfers, I am aware that computer equipment was used to generate, store, and print documents used in the securities fraud and wire fraud scheme. There is reason to believe that there is one or more computers or computer systems currently located at the PREMISES.

83. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes

described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any electronic storage medium located at the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the

innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and

have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether

data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

84. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on electronic storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence

of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

85. *Unlocking devices*. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the

use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some

cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

86. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant applied for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later

review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

87. While it appears that SPIVAK is using the PREMISES and USLG to commit securities fraud, US Lighting Group, Inc. ("the Company") is a functioning company that may conduct legitimate business. The seizure of the Company's computers may limit the Company's ability to conduct its legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. However, where seizure would reduce the length of the disruption, officers will seize the computers for off-site examination and copying and return the computers as noted below. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

CONCLUSION

88. I submit that this affidavit supports probable cause that violations of Title 15, United States Code, Sections 78j(b), 78ff, Title 17; Code of Federal Regulations, Section 240.10b-5, Title 18, United States Code, Sections 371 have been committed by PAUL SPIVAK, and others, and that evidence, fruits and instrumentalities pertaining to said offenses as set forth

in Attachment B are presently located at the subject PREMISES, more specifically described in Attachment A, both of which are attached hereto and incorporated herein by reference.

Respectfully submitted,

Anthony Fry
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone, on this 07th day of June 2021.

Jonathan D. Greenberg
United States Magistrate Judge